



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/889,524	02/28/2002	Dan Butnaru	09669/004001	5237
22511	7590	04/07/2005	EXAMINER	
OSHA & MAY L.L.P. 1221 MCKINNEY STREET SUITE 2800 HOUSTON, TX 77010			HENNING, MATTHEW T	
			ART UNIT	PAPER NUMBER
			2131	

DATE MAILED: 04/07/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/889,524	BUTNARU ET AL.	
	Examiner	Art Unit	
	Matthew T Henning	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 20 January 2005.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 2-23 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 2-23 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 28 February 2002 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

This action is in response to the communication filed on 1/20/2005.

DETAILED ACTION

1. Claims 2-23 have been examined.
2. All objections and rejections not set forth below have been withdrawn.

Title

3. The title of the invention is acceptable.

Priority

4. The application is a 371 of PCT/FR00/00099 filed 1/18/2000 claiming priority to France application 99/00462 filed on 01/18/1999.
5. The effective filing date for the subject matter defined in the pending claims in this application is 01/18/1999.

Information Disclosure Statement

6. The information disclosure statement (IDS) submitted on 02/28/2002 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the examiner is considering the information disclosure statement.

Drawings

7. The drawings filed on 02/28/2002 are acceptable for examination proceedings.

Specification

8. Applicant is reminded of the proper language and format for an abstract of the disclosure.

The abstract should be in narrative form and generally limited to a single paragraph on a separate sheet within the range of 50 to 150 words. It is important that the abstract not exceed 150 words in length since the space provided for the abstract on the computer tape used by the printer is limited. The form and legal phraseology often used in patent claims, such as "means" and "said," should be avoided. The abstract should describe the disclosure sufficiently to assist readers in deciding whether there is a need for consulting the full patent text for details.

The language should be clear and concise and should not repeat information given in the title. It should avoid using phrases which can be implied, such as, "The disclosure concerns," "The disclosure defined by this invention," "The disclosure describes," etc.

9. The abstract of the disclosure as amended is objected to because

Lines 5 and 8 contain legal phraseology ("said"), which must be removed.

Correction is required. See MPEP § 608.01(b).

Claim Rejections - 35 USC § 102

10. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

11. Claims 2-11, and 13-23 are rejected under 35 U.S.C. 102(b) as being anticipated by Moriyasu et al. (US Patent Number 5,651,066) hereinafter referred to as Moriyasu.

12. Claim 20 recites a method for customizing a set of several second security units (See Moriyasu Fig. 3 and Field of the Invention), comprising:

secure downloading of an application key from a first security unit of a central processing unit to said set of second security units (See Moriyasu Fig. 3 and Field of the Invention), said first unit and second units each comprising at least one memory (See Moriyasu Col. 7 Paragraph 8 wherein it was implied that the management units had memory because keys were stored there), wherein the method further comprises for each second unit in said set:

on each downloading (See Moriyasu Fig. 10), computing an operation key ($K3' + K4$) in the first unit based on information specific to the second unit ($K3$), a transport key ($K4$), and a diversification algorithm (Multi-Value Function) (See Moriyasu Col. 8 Paragraph 6), said transport key residing within the memory of the first security

Art Unit: 2131

unit, said memory being non volatile (See Moriyasu Col. 10 Paragraph 8 and Col. 7 Paragraph 8 wherein it was implied that the keys were stored in non-volatile memory in order for them to be used to encrypt and decrypt the multiple communications);

encrypting the application key in the first unit based on information comprising said operation key and an encryption algorithm (See Moriyasu Col. 8 Lines 42-50);

sending data comprising the encrypted application key to the second unit (See Moriyasu Col. 8 Lines 42-50);

on each downloading, computing an operation key ($K3'+K4$) in the second unit based on information specific to the second unit ($K3$), the transport key ($K4$) and the diversification algorithm (Multi-Value Function) (See Moriyasu Col. 8 Paragraph 5), the same transport key residing in the non-volatile memory of each second security unit of said set (See Moriyasu Col. 10 Paragraph 8 and Col. 7 Paragraph 8 wherein it was implied that the keys were stored in non-volatile memory in order for them to be used to encrypt and decrypt the multiple communications), said operation key not being stored within the memory of said second unit (See Moriyasu Col. 8 Paragraph 8 and Fig. 10); and

decrypting the encrypted application key in the second unit based on information comprising said operation key and a decryption algorithm which is the inverse of the encryption algorithm (See Moriyasu Col. 8 Paragraph 8).

13. Claim 2 recites sending information specific to the second unit to the first unit before computing the application key in the first unit (See Moriyasu Col. 8 Paragraph 2 and Fig. 10).

14. Claim 3 recites sending a random number provided by the second unit to the first unit, before encrypting the application key in the first unit (See Moriyasu Fig. 10 Element K3 and AP Key Request Signal and Col. 7 Paragraph 9 – Col. 8 Paragraph 2).

15. Claim 4 recites sending information pertaining to an application key to the first unit, before encrypting the application key within said first unit (See Moriyasu Col. 8 Paragraph 4).

Art Unit: 2131

16. Claim 5 recites choosing the application key to be encrypted based on said information pertaining to an application key (See Moriyasu Col. 8 Paragraph 4).

17. Claim 6 recites that the encryption of an application key intended for a second unit is unique (See Moriyasu Col. 8 Paragraph 6 wherein the encryption is based on random numbers and is therefore unique).

18. Claim 7 recites verifying integrity of the data, wherein verifying the integrity of the data comprises verifying the encrypted application key (See Moriyasu Fig. 10 and Col. 7 Paragraph 9 – Col. 8 Paragraph 8 wherein the exchanging of keys to create a key ($K3'+K4$) for AP key transmission inherently provided integrity verification of the received application key).

19. Claim 8 recites sending information pertaining to an application key to the second unit, before decrypting the encrypted application key within said second unit of said set (See Moriyasu Col. 8 Paragraphs 6-8 and Fig. 10).

20. Claim 9 recites storing within the second unit, after decrypting the encrypted application key, said key within said second unit (See Moriyasu Col. 1 Field of the Invention wherein the point of the invention was to distribute keys to terminals, which implied that the keys would be stored).

21. Claim 10 recites that storing of the application key within the second unit is done based on information pertaining to an application key (See Moriyasu Col. 8 Paragraph 8 and rejection of claim 9 above, wherein it was inherent that storing the AP key was based on the AP key).

22. Claim 11 recites verifying that the application key is authentic (See Moriyasu Fig. 10 and Col. 7 Paragraph 9 – Col. 8 Paragraph 8 wherein the exchanging of keys to create a key ($K3'+K4$) for AP key transmission inherently provided validation that the received key was authentic).

23. Claim 13 recites that the memory comprises a rewritable memory (See Moriyasu Col. 7 Paragraph 8 wherein it was implied that the storage was rewritable in order to write the keys to the storage unit).

Art Unit: 2131

24. Claim 14 recites that a second unit comprises several application keys (See Moriyasu Col. 11 Paragraph 3 wherein a user purchases a CD-ROM and installs it on the users personal terminal. It was inherent that if a user purchased several CD-ROMs and then installed them, the user's terminal would have had multiple keys).

25. Claim 15 recites that the first unit comprises several application keys (See Moriyasu Col. 7 Paragraph 8).

26. Claim 16 recites that after encrypting the application key, erasing the operation key temporarily saved within the second volatile memory of the first unit (See Moriyasu Col. 8 Paragraph 6 wherein it was implied that the key used for encrypting the AP key was erased after encryption because it was not stored in the key management unit).

27. Claim 17 recites that after decrypting the application key, erasing the operation key temporarily saved within the second volatile memory of the first unit (See Moriyasu Col. 8 Paragraph 8 wherein it was implied that the key used for decrypting the AP key was erased after decryption because it was not stored in the key management unit).

28. Claim 18 recites sending the random information, information pertaining to an application key and information specific to the second unit to the first unit by means of a first single command (See Moriyasu Fig. 10 AP Key Request Signal and Col. 7 Paragraph 9 – Col. 8 Paragraph 2).

29. Claim 19 recites sending the encrypted application key and the information pertaining to an application key to the second unit by means of a single second command (See Moriyasu Col. 8 Lines 42-50).

30. Claim 21 is rejected for the same reasons as claim 18 above.

31. Claim 22 is rejected for the same reasons as claims 18 and 4 above.

32. Claim 23 recites sending the encrypted application key and the information pertaining to an application key to the second unit by means of a single second command (See Moriyasu Fig. 10 AP Key Distribution Signal and Col. 8 Lines 42-50).

Claim Rejections - 35 USC § 103

33. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

34. Claim 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over Moriyasu as applied to claim 20 above, and further in view of Mollier.

Moriyasu disclosed a system for providing a software key from a remote location to a user terminal (See rejection of claim 20 above), but failed to disclose the system comprising a smartcard.

Mollier teaches a system in which a smartcard, able to provide a key to allow unscrambling of a software program, is provided to a paying user (See Mollier Col. 2 Paragraphs 3-10 and Fig. 1)

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the smartcard of Mollier to the key transferring method of Moriyasu. This would have been obvious because the ordinary person skilled in the art would have been motivated to provide a way for a supplier to rent programs to a user.

Response to Arguments

35. Applicant's arguments filed 1/20/2005 have been fully considered but they are not persuasive.

36. Applicants argue primarily that:

- a. Moriyasu failed to disclose a transport key.
- b. Moriyasu failed to disclose storing a transport key in non-volatile memory.
- c. Moriyasu failed to disclose “using information pertaining to an application key”.

37. In response to applicant’s argument a. that Moriyasu failed to disclose a transport key, the examiner does not find the argument persuasive. Moriyasu clearly disclosed a transport key as shown by Fig. 10 element K4 and K4 is clearly present in both units prior to communicating the application key, which can be seen clearly in Fig. 10.

38. The argument that K4 is not present prior to the communication between the first and second units is also not persuasive. In response to applicant's argument that the references fail to show certain features of applicant’s invention, it is noted that the features upon which applicant relies (i.e., the transport key being present in both units prior to communication between the units) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). Therefore, the examiner has maintained the rejections presented above.

39. In response to the applicants’ argument b. that Moriyasu did not disclose the transport key being stored in non-volatile memory, the examiner does not find the argument persuasive. Moriyasu disclosed a transport key K4 being created at the key center, to be used in place of the public/secret key pair (K2e/K2d) of the embodiment of Fig. 6, and transmitting K4 to the user terminal (See Moriyasu Col. 10 Line 53 – Col. 11 Line 3). Moriyasu further disclosed that K4 was used more than once, at different times in both the user terminal and the key center (See

Art Unit: 2131

Moriyasu Fig. 10 Elements 63-64 and 22-24, Col. 10 Line 53 – Col. 11 Line 3 and Col. 8 Lines 8-60 wherein the public and secret keys referenced by Fig. 6 were replaced by K4). Moriyasu further disclosed storing the public key in the key management unit of the user terminal and the secret key in the key management unit of the key center (See Moriyasu Col. 7 Lines 56-62).

Therefore, because K4 was replacing the public/secret key pair in the embodiment of Fig. 10, K4 was stored in the key management units of the terminals and of the center.

40. Furthermore, as to the argument that the key would not need to be stored in non-volatile memory in the embodiment of Fig. 10, it was inherent that the key was stored at both the terminal and the center. This was inherent because K4 was used at different times throughout the communications. This can be seen from Fig. 7, which refers to the steps performed for the embodiment of Fig. 6, and therefore for the steps of the embodiment of Fig. 10 with the public and secret keys replaced by K4. As can be seen in Fig. 7, the key center generated and used K4 in step 504, 506, 507, and 509. It should be noted that between steps 504 and 506, the message containing K4 is sent from the center to the terminal, at which point the terminal deciphers K4, performs a multi-value operation on K3, to get K3', enciphers K4 and K3', and sends the result of the encryption to the center. It should also be noted that this was not an instantaneous process and therefore K4 must have been stored at the key center between the steps 504 and 506. By the same reasoning, it was inherent that K4 was stored at the user terminal between steps 505 and 510.

41. Furthermore, the only storage disclosed by Moriyasu was the key management units, which stored keys (See Moriyasu Col. 7 Lines 19-62). It was therefore inherent that K4 was stored in the key management units at the terminals and the key center. It was also inherent that

Art Unit: 2131

this storage was non-volatile storage. This was due to the fact that the keys stored in the key management units included long-term keys that were stored well in advance to the key downloading method of Fig. 10 (See Moriyasu Col. 7 Lines 56-62 and Col. 11 Lines 7-61), and if the memory was volatile the keys could have been lost and the applications would have become un-decipherable.

42. Because of the reasons discussed above, Moriyasu did disclose storing the transport keys in non-volatile memory, and therefore the examiner has maintained the rejections presented above.

43. Regarding applicant's argument c. that Moriyasu failed to disclose "using information pertaining to an application key", the examiner does not find the argument persuasive. Moriyasu did disclose using the information to choose the application key and transferring the information between the terminal and the center through a single command (See Moriyasu Col. 8 Paragraph 4 and Fig. 10). Moriyasu further disclosed sending information pertaining to an application key to the terminal from the center by a single command before decrypting the encrypted application key at the center (See Moriyasu Fig. 10 and Col. 8 Paragraph 6 wherein the encrypted application key falls within the scope of information pertaining to the application key). Moriyasu further disclosed storing the application key based on information pertaining to the application key (See Moriyasu Col. 8 Paragraph 8 wherein it was inherent that deciphered the application key was stored or it could not have been used to decrypt the application program, and further the key must have been stored based on the information that was the key). As such, the examiner has maintained the rejection presented above.

Conclusion

44. Claims 2-23 have been rejected.

45. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- i. Epstein (US Patent Number 5,517,567) disclosed a method for providing remote units with a security key, only deviating from the claims in minor, obvious details.
- ii. Garguilo et al. (US Patent Number 4,935,961) disclosed a method for synchronizing cryptographic keys involving key encrypting keys.
- iii. White et al. (US Patent Number 5,199,072) disclosed shows that it was well known in the art at the time of invention to store keys in non-volatile memory.

46. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the mailing date of this final action.

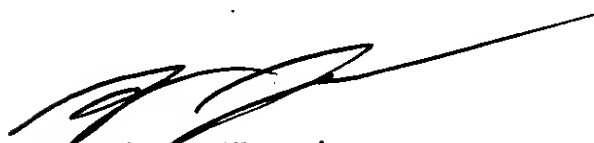
Art Unit: 2131

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew T Henning whose telephone number is (571) 272-3790.

The examiner can normally be reached on M-F 8-4.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Matthew Henning
Assistant Examiner
Art Unit 2131
4/1/2005



AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100